DEPARTMENT OF VETERANS AFFAIRS
Office of Information and Technology
Office of Information Security
Risk Management and Incident Response
Incident Resolution Team

Monthly Report to Congress of Data Incidents

September 2 - September 29, 2013

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094111	Mishandled/ Misused Physical or Verbal Information	VISN 23 St. Cloud, MN	9/2/2013	9/9/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596339	9/2/2013	INC000000310717	N/A	No	N/A	1	

Incident Summary

Veteran A received Veteran B's full SSN and medical information. A provider from the facility gave it to Veteran A by mistake.

Incident Update

09/03/13:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 100 Mis-Handling incidents this reporting period. Because of repetition, the other 99 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The provider was re-educated on policies and procedures and the training and awareness of handling patient information.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094143	Mishandled/ Misused Physical or Verbal Information	VBA Atlanta, GA	9/3/2013	9/5/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596374	9/3/2013	INC000000310869	N/A	N/A	N/A	1	

Incident Summary

Veteran A stated that he received a letter belonging to Veteran B attached with his decision letter. Veteran A advised that the letter was mailed from the Regional Office (RO). The letter included Veteran B's name, address, dates of military service and full SSN.

Incident Update

09/03/13:
Veteran B will be sent a letter offering credit protection services.

NOTE: There were a total of 96 Mis-Mailed incidents this reporting period. Because of repetition, the other 95 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents, Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The employee was counseled and completed the Privacy and Information Security Awareness and Rules of Behavior Training in the Talent Management System (TMS). The employee was reminded to review all documents before mailing and will upload the correct files into Veterans Benefits Management System (VBMS) to avoid future mis-mailing.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094179	Missing/Stolen Equipment	VISN 10 Cleveland, OH	9/4/2013	9/24/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596410	9/4/2013	INC000000311022	N/A	N/A	N/A		141

Incident Summary

A VA employee who works for Home Based Primary Care (HBPC) in Painesville, OH reported that his government vehicle, which was parked at the State Street Clinic, was broken into between 4:00 PM 09/03/13 and 7:40 AM 09/04/13. There was a government laptop in the vehicle and it was stolen. The laptop is encrypted however the VA employee wasn't sure if there was patient information stored on the laptop. It was reported to the VA Police.

Incident Update

09/09/13:
The laptop was encrypted. It was last seen at 4:00 PM on 09/03/13. It was used by a HBPC employee to access Outlook email and CPRS for charting patient encounters. There was no personally identifiable information (PII) or protected health information (PHI) stored on the laptop. It was in the car because the employee works outreach and drives to the patients' homes. He was not on duty at the time. A computer bag, an electrical power source and a trip ticket binder were also taken. One, or possibly two, patients' medication reconciliation forms were also taken. The employee can reconstruct what was on those papers.

09/17/13:
The laptop and bag were recovered on 09/15/13 in a suspect's residence. In the bag were 21 pages of documents. There were 141 patients' full names, last four of SSNs, home addresses and home telephone numbers. The Privacy Officer (PO) requested the ticket be re-opened this morning in light of the new evidence. Previously, the employee stated there was only two patients' information in the bag. The 141 patients will receive HIPAA notification letters.

Resolution

The Police report was completed. The employee has been interviewed and counseled on securing VA assets.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094241	Missing/Stolen Equipment	VISN 04 Philadelphia, PA	9/5/2013		High

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596470	9/5/2013	INC000000311380	N/A	N/A	N/A		80

Incident Summary

During an IT equipment inventory, it was discovered that a laptop from the Audiology Department was missing. This laptop was on loan to the VA by a vendor (over 7 years ago). The laptop was a standalone biomedical device and attached to a hearing aid programming station used for reprogramming and adjusting hearing aids.

Incident Update

09/05/13:
It was not encrypted because it was the property of the contractor, who loaned it to the VA over seven years ago. The laptop did have the full name, last four of SSN and hearing aid data for 80 Veterans stored on it.

09/09/13:
The laptop still has not been located. Notification letters will be sent to 80 patients.

09/13/13:
VA Police are still investigating this incident

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094283	Missing/Stolen Equipment	WASHINGTON DC-VACO - 101 Washington, DC	9/5/2013	9/30/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596514	9/5/2013	INC000000311568	N/A	N/A	N/A		

Incident Summary

VA Office of Management is reporting two VA owned new unencrypted laptops were stolen while under VACO Service Delivery Engineering (SDE) staff possession.

Incident Update

09/06/13:
On 09/05/13 at approximately 5:54 PM, it was reported that two VA owned laptops were stolen from the VA Office of Management Service while under VACO SDE staff possession. The two laptops that were stolen are new Dell Latitudes with docking stations and accessories. According to the Report of Survey (RoS), the Supervisor gave an IT technician four special ordered Dell Latitude laptops to have imaged with four docking stations, four power adapters, and additional items that came with each laptop. Two of the laptops were completed and returned to the customer and two were left with the IT Specialist to complete. The IT Specialist went on annual leave from 08/16/13 to 08/26/13, leaving the laptops on his desk and upon his return, the laptops, docking stations, and accessories were no longer in the technician's cubicle. The Supervisor inquired about the laptops on 08/26/13 and was told of the missing laptops. Two days were given to see if they would turn up. An email was received from the Supervisor on 08/29/13 that the laptops were missing. Another two days were given to see if they would turn up. On 09/03/13, the IT technician was contacted and he reported that they have not turned up. The laptops were new and not encrypted and they did not contain any VA information.

09/30/13
The missing laptops were reported to VA Police and VACO SDE staff will replace devices that were stolen. No personally identifiable information (PII) was on the stolen equipment.

Resolution

A VA Police report has been filed for missing laptop and VACO SDE will supply replacements.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094694	Mishandled/ Misused Physical or Verbal Information	VISN 07 Montgomery, AL	9/16/2013	10/7/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0596901	9/16/2013	INC000000313874	N/A	No	N/A	61	

Incident Summary

Veteran A called to report that he received a three page document that contained a list of several other Veterans' names and full SSNs, along with his appointment reminder.

Incident Update

09/23/13:
The Privacy Officer (PO) talked to the Veteran and mailed him a stamped envelope to return the list to the VA. On 09/20/13 the PO called him again. He stated that he mailed the envelope to the VA on 09/19/13. The staff who accidentally sent him the appointment reminder does not know what type of list he could have received.

09/24/13:
The Veteran was mailed his appointment reminder, along with other extraneous pages of Veterans' names and SSNs (61 names total). Someone was trying to print future appointment letters but did not have it set up properly. The Veteran mailed it promptly back to the VA. The 61 Veterans will receive a letter offering credit protection services.

Resolution

The Clinic has changed procedures for mailing appointment reminders. Other employees are involved in the process. Employees have been reminded to take extra precautions to ensure information is mailed to the correct patients.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094860	Mishandled/ Misused Physical or Verbal Information	VHA CMOP Charleston, SC	9/19/2013	9/27/2013	Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597057	9/19/2013	INC000000314847	N/A	N/A	N/A		1

Incident Summary

Patient A received a prescription intended for Patient B. Patient B's name and type of medication was compromised. Patient A reported the incident to the Central Alabama Healthcare VA Medical Center and a replacement has been requested for Patient B. The Charleston Consolidated Mail Outpatient Pharmacy (CMOP) investigation concludes that this was a CMOP packing error. The CMOP employees will be counseled and retrained in proper packing procedures.

Incident Update

09/20/13:
One patient will be sent a notification letter.

NOTE: There were a total of 2 Mis-Mailed CMOP incidents out of 5,986,697 total packages (9,093,793 total prescriptions) mailed out for this reporting period. Because of repetition, the other 1 is not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In both incidents, Veterans will receive a notification letter.

Resolution

The CMOP employees was counseled and retrained in proper packing procedures.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000094915	Missing/Stolen Equipment	VISN 03 Bronx, NY	9/20/2013	10/3/2013	Low

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597102	9/20/2013	Non-Event See	N/A	N/A	N/A		

Incident Summary

A VA employee lost a non-VA owned laptop used for non-sensitive VA research.

Incident Update

09/23/13:
The laptop contained published research reports, but no protected health information or personally identifiable information.

10/3/13:
The employee left the Apple MacBook Air laptop in the Copenhagen airport at the gate. He has made multiple calls to the airport, but they have not found it. He reported the loss to VA Police also. The laptop did not have any PHI on it. He did not store any research data on the laptop, as it is all stored on a server. The laptop was never attached to the VA network. It did contain some manuscript preparation documents, external e-mail, and presentations. His interpretation of data was done on the computer but no data was ever stored there. The laptop was purchased by the research foundation with funds from a DoD grant. It was password protected.

Resolution

The laptop was never connected to the VA network and no VA sensitive/patient data was ever stored on laptop.

Security Privacy Ticket Number	Incident Type	Organization	Date Opened	Date Closed	Risk Category
PSETS0000095109	Mishandled/ Misused Physical or Verbal Information	VISN 02 Syracuse, NY	9/25/2013		Medium

VA-NSOC Incident Number	Date US-CERT Notified	US-CERT Case Number	Date OIG Notified	Reported to OIG	OIG Case Number	No. of Credit Monitoring	No. of Loss Notifications
VANSOC0597294	9/25/2013	INC000000316258	N/A	N/A	N/A		80

Incident Summary

The Privacy Officer (PO) was contacted by the VISN 2 Coding Coordinator regarding patient information found unsecured. The Coding Coordinator stated that she found a list containing the names, last 4 digits of the SSNs, and emergency department visit dates of 80 patients in the parking lot of the Buckley Road VA Office building. The list was found upon the Coding Coordinator's return from lunch and was not present when leaving. The Coding Coordinator retrieved the list and secured it in her office until it was turned over to the Privacy Officer (PO). The PO is currently investigating where the list was generated from to determine how it was left in the parking lot so further correction can be taken as needed to prevent future occurrences.

Incident Update

09/30/13:
The list was left unsecured in an area accessible to the general public for several hours. Notification letters will be sent to the 80 patients involved.

Total number of Internal Un-encrypted E-mail Incidents	83
Total number of Mis-Handling Incidents	100
Total number of Mis-Mailed Incidents	96
Total number of Mis-Mailed CMOP Incidents	2
Total number of IT Equipment Inventory Incidents	1
Total number of Missing/Stolen PC Incidents	2
Total number of Missing/Stolen Laptop Incidents	7 (3 unencrypted)
Total number of Lost BlackBerry Incidents	19
Total number of Lost Non-BlackBerry Mobile Devices (Tablets, iPhones, Androids, etc.) Incidents	0